UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/688,397 | 10/16/2003 | Graeme John Proudler | B-5268 621375-8 | 1309 |

7590 04/30/2008

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

| EXAMINER | |
|---|---|
| MORAN, RANDAL D | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2135 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 04/30/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Application Number: 10/688,397
Filing Date: October 16, 2003
Appellant(s): PROUDLER, GRAEME JOHN

Richard P. Berg
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed 2/4/2008 appealing from the Office action mailed 9/5/2007.

**(1) Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is correct.

**(4) Status of Amendments After Final**

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

| | | |
|---|---|---|
| 2002/0059286 | Challener | 5-2002 |
| 5,796,839 | Ishiguro | 5,796,839 |

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

***Claim Rejections - 35 USC § 103***

**Claims 35-42, 44, 46-49** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Challener (US 2002/0059286)** in view of **Ishiguro (US 5,796,839)**.

The final rejection inadvertently omitted Ishiguro in the heading under 35 U.S.C. 103. The heading should have included **Ishiguro (US 5,796,839)**, and is hereby corrected.

Considering **Claims 35-49,** Challener discloses a secure key-handling unit arranged to store a storage root key that forms the root node of a tree- structured node hierarchy (abstract) the non-leaf nodes of which, other than the root node, each comprise, in encrypted form, a key used to encrypt the or each of its child nodes ([0021]), and insecure storage for storing the hierarchy nodes other than the root node [0021] lines 6-8); a decrypted-access arrangement arranged to restrict decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key ([0021]).

Challener does not explicitly disclose the key-handling unit comprising: a memory for storing a current decryption-root key; a current-decryption-root setting arrangement for storing in said memory, in decrypted form, the key of a selected non-leaf node of said hierarchy to serve as said

current decryption-root key, the current-decryption-root setting arrangement enabling the selected non-leaf node to be changed.

Ishiguro discloses a the key-handling unit comprising: a memory for storing a current decryption-root key (column 6- lines 6-10); current-decryption-root setting arrangement for storing in said memory (column 5- lines 20-29), in decrypted form (column 7- lines 57-66), the key of a selected non-leaf node of said hierarchy to serve as said current decryption-root key (column 5- lines 20-29 and 42-53, column 6- lines 30-34, column 7- lines 34-66), the current-decryption-root setting arrangement enabling the selected non-leaf node to be changed (column 4- lines 60-67, column 5- lines 1-13, the "work key" may be changed relative to how much information the user is authorized to access).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Challener by the current decryption-root arrangement as taught by Ishiguro to provide a decoding apparatus in which encryption keys can be managed with ease (Ishiguro- column 2- lines 10-11).

Considering **Claim 36,** the combination of Challener and Ishiguro discloses the setting arrangement for changing the current root node is enabled to do so only upon a predetermined set of at least one condition being met (Challener- [0007], Ishiguro- column 7- lines 43-66).

Considering **Claim 37,** the combination of Challener and Ishiguro discloses at least one predetermined condition comprises the receipt by the key handling unit of an authorization value indicative of particular digital data (Ishiguro- column 7- lines 39-42).

Considering **Claim 38,** the combination of Challener and Ishiguro discloses authorization value is a digest of a protected process associated with the node that is intended to be the new selected non-leaf node (Challener- p.5 right column, lines 14-17, Ishiguro- column 4 lines 25-34).

Considering **Claim 39,** the combination of Challener and Ishiguro discloses at least one predetermined condition comprises that a protected process associated with the node that is intended to be the new selected non-leaf node is about to be run by the computing platform (Challener- [0021], if you are attempting to migrate keys and access them, you are also intending to unlock the nodes and run the process, Ishiguro- column 5- lines 14-19, column 8- lines 1-5).

Considering **Claim 40,** the combination of Challener and Ishiguro discloses at least one predetermined condition comprises that any other currently-activated processes running on the apparatus are benign (Challener- Fig. 9).

Considering **Claim 41,** the combination of Challener and Ishiguro does not explicitly disclose at least one predetermined condition comprises that the key-handling apparatus is requested to change the current root node by a root of trust of the apparatus.
Official notice is taken that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Challener and Ishiguro by the root change request coming from a root of trust as is well known in the art for the benefit of having a set of unconditionally trusted functions that must work properly no matter what software is executing on the platform, in order to be immune to software attacks. Ideally, it should also be immune to physical attack, to avoid the need to trust an owner or user of a platform.

Considering **Claim 42,** the combination of Challener and Ishiguro discloses upon start up of the computing platform, the node at the head of the hierarchy forms said selected non-leaf node (Challener- Fig. 5- item 501, upon start-up, the storage root key is always considered the current root node, Ishiguro- column 3- lines 30-39).

Considering **Claim 44,** the combination of Challener and Ishiguro discloses the key-handling unit is arranged to always hold securely the node at the head of the hierarchy, in unencrypted form (Challener- [0021] lines 8-11, Ishiguro- column 7- lines 63-66).

Considering **Claim 46,** the combination of Challener and Ishiguro discloses the key-handling unit is arranged to indicate the current root node by signing a value associated with the node using an identity key associated with the key-handling unit (Challener- [0028], [0029], the non-migratable storage key is used to create a signature that would be used to identify it to the chip, Ishiguro- column 7- lines 39-46).

Considering **Claim 47,** the combination of Challener and Ishiguro discloses the key-handling unit is so arranged that only a particular type of key node (Challener [0021] lines 24-27, only the key set to be migrated can be used as the current root node) herein a dynamic key node, can be used as the current root node in addition to the node at the head of the hierarchy (Challener- Fig 5, the storage root key can be used as the root as well as the migratable key (i.e. the dynamic root), Ishiguro- column 4- lines 60-67, column 5- lines 1-13).

Considering **Claim 48,** the combination of Challener and Ishiguro discloses the key-handling apparatus is arranged, upon receipt of a corresponding command, to generate a dynamic root node as a node of said key hierarchy (Challener- [0007]).

Considering **Claim 49**, the combination of Challener and Ishiguro disclose the setting arrangement is arranged to permit the selected non-leaf node to be changed to one associated with a protected process upon receipt by the key-handling unit of a reliable indication that a mechanism expected to resist subversion will attempt to enforce appropriate access restrictions on that node and any descendent nodes, the key of the non-leaf node associated with said protected process being available for use in relation to the protected process upon becoming the decryption root key (Ishiguro- column 7- lines 39-66).

**(10) Response to Argument**

Group #1: **Claims 35-42, 44, 46-49.**

The final rejection inadvertently omitted Ishiguro in the heading under 35 U.S.C. 103. The heading should have included **Ishiguro (US 5,796,839)**, and is hereby corrected.

Appellant agrees that Challener discloses "the decrypted access arrangement" (Appeal brief- p. 6, ¶ 2). Challener [0021] discloses:

> "A storage root key is a private, 2048 bit RSA key created and stored in non-volatile memory in a TPM. This key is used to store other keys (referred to as children keys), as other keys can be wrapped with the public portion of the storage root key, at which point only the chip can decrypt them. A platform key 102 is a migratable private 2048 bit RSA key wrapped by the storage root key 101 and used as a root for other migratable keys. For example, user keys 103 (children of the platform key) may be wrapped with the public portion of a platform key 102. At

> this point, in order to decrypt a user key 103 into the chip, first the platform key 102 has to be loaded into the TPM, so the TPM knows its private key, and then the user key 103 is loaded into the TPM (which may require use of user authorization data of the platform key 102) using that private key. When upgrading hardware, it is only the migratable key that typically will need to be migrated, as all other migratable keys will exist below it. Thus, migrating this key to a new platform also effectively migrates all the keys below it. The user key 103 is a migratable private 2048 RSA key wrapped by the platform key 102 and used as a root for all of a user's migratable keys. It typically will be used to store both symmetric and private signing keys belonging to the user. When a signing key is needed, it would be required to load the user key 103, which would require the need to load the platform key 102, from the storage root key 101. The need to load all these keys will require a relatively significant amount of time when such keys are 2048-bit RSA keys."

Challener explicitly discloses a decrypted access arrangement (i.e. the storage root key being used to decrypt all leaf nodes below it). The Challener reference is not relied upon to show the ability to change the current-decryption-root key. As noted by the appellant (Appeal Brief- p.6, ¶ 2), the storage root key of Challener provides the chain of decryption for the hierarchy of nodes. Therefore, Challener in view of Ishiguro explicitly discloses the decrypted access arrangement utilizing a chain of decryption from the newly selected current-decryption-root key.

Appellant agrees that Ishiguro discloses "the current-decryption-root setting arrangement" (Appeal brief- p. 8, ¶ 3). Appellant argues the examiners analysis to come to this conclusion. Ishiguro- column 5- lines 20-56, column 6- lines 30-34 discloses:

> "an encryption key of a proper generation (hierarchy) is selected from hierarchized encryption keys shown in FIG. 2 at a step S1 and the selected encryption key is set to a work key. Then, control goes to a step S2, wherein a string of predetermined numerals and characters is set to a magic number, the magic number is encrypted by the work key obtained at the step S1 and the encrypted magic number obtained by the encryption is recorded on a predetermined portion of a DVD 1 as shown in FIG. 4, for example."

> "A work key generating circuit 53 selects an encryption key of a proper generation (hierarchy) from the hierarchized encryption keys shown in FIG. 2 and supplies the selected encryption key to the encryption circuits 51, 52 as a work key. The encryption key 52 encrypts the supplied magic number by using the work key supplied thereto from the work key generating circuit 53.

> Then, encrypted magic number thus obtained by encryption is supplied to a recording apparatus 54. The encryption circuit 51 encrypts the supplied plain text data by using the work key and supplies the encrypted information to the recording apparatus 54. The recording apparatus 54 records the encrypted information and the encrypted magic information on the predetermined positions of the DVD 1 as shown in FIG. 4."
>
> "a master key is read out from the memory 12 of the IC chip 11 and set to a selection key (k). Then, this selection key (k) is supplied to the decoding circuit 14. The selection key (k) expresses an encryption key that is selected at present."

Ishiguro explicitly discloses a current-decryption-root setting arrangement (i.e. an encryption key of a proper generation (hierarchy) is selected from hierarchized encryption keys selected encryption key is set to a work key). Ishiguro goes on to further disclose a master key being read out from and set to a selection key. The selection key (k) expresses an encryption key that is selected at present. The selection key is then set to the previously described work key (Ishiguro- column 6- lines 61-64, Fig. 8). Therefore, Challener in view of Ishiguro explicitly discloses the current-decryption-root setting arrangement as agreed by the appellant (Appeal brief- p. 8, ¶ 3).

Appellant argues that the combination of Challener and Ishiguro fails to teach "a decrypted-access arrangement to restrict decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key". Appellant agrees that Challener discloses a decrypted-access arrangement (Appeal brief- p. 6, ¶ 2). The storage root key being used as the head of the chain of decryption used to restrict decrypted access to the hierarchy nodes. The appelant agrees that Ishiguro discloses the current-decryption-root setting arrangement (Appeal brief- p. 8, ¶ 3). Therefore, once the selection key is set to the work key (Ishiguro- column 6- 61-64), the current-root-decryption key becomes the head of the chain of decryption (Challener- [0021]). Therefore, the combination of Challener and Ishiguro explicitly discloses a decrypted-access arrangement to restrict

decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key.

Appellant argues that the examiner has not provided a reasonable rationale for combining the teachings of Challener and Ishiguro. In response to appellant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, one of ordinary skill in the art would at the time of the invention, would have been motivated to combine the decrypted-access arrangement as taught by Challener with the current-decryption-root setting arrangement as taught by Ishiguro to provide a decoding apparatus in which encryption keys can be managed with ease (Ishiguro- column 2- lines 10-11, column 5- lines 1-13). All of the components (i.e. decrypted access arrangement and current-decryption-root setting arrangement) are known within the Challener and Ishiguro. The combination of the decrypted-access arrangement of Challener and the current-decryption-root of Ishiguro would have the yielded the predictable result of key hierarchy in which keys can be managed with ease.

**(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Art Unit: 2135

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/R. D. M./

Examiner, Art Unit 2135

Conferees:

Christopher Revak

/Christopher A. Revak/

Primary Examiner, Art Unit 2131

/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135